ATTACHMENT IV

OPERATIONS SUPPORT SYSTEMS

APPENDIX OSS
(ACCESS TO OPERATIONS SUPPORT SYSTEMS FUNCTIONS FOR FIXED WIRELESS SERVICE)

1.   INTRODUCTION

1.1   This Appendix sets forth terms and conditions for nondiscriminatory access to Operations Support Systems (OSS) "functions" provided by the applicable SBC Communications Inc. (SBC) owned Incumbent Local Exchange Carrier (ILEC) and necessary for the ordering of Local Number Portability ("LNP"), Directory Listings ("DL") and E911 that are requested by AWS and required for the provision of fixed wireless service, under the Agreement, in substantially the same technical manner that AWS or one of its affiliated wireless companies provides fixed wireless in one or more states as of the effective date of this Appendix.

1.2   SBC Communications Inc. (SBC) means the holding company which owns the following ILECs: Illinois Bell Telephone Company, Indiana Bell Telephone Company Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Pacific Bell Telephone Company, The Southern New England Telephone Company, Southwestern Bell Telephone Company and/or Wisconsin Bell, Inc. d/b/a Ameritech Wisconsin.

1.3   SBC-13STATE - As used herein, SBC-13STATE means the applicable above listed ILEC(s) doing business in Arkansas, California, Connecticut, Illinois, Indiana, Kansas, Michigan, Missouri, Nevada, Ohio, Oklahoma, Texas, and Wisconsin.

1.4   SBC-12STATE - As used herein, SBC-12STATE means the applicable above listed ILEC(s) doing business in Arkansas, California, Illinois, Indiana, Kansas, Michigan, Missouri, Nevada, Ohio, Oklahoma, Texas, and Wisconsin.

1.5   SBC-8STATE - As used herein, SBC-8STATE means an applicable above listed ILEC(s) doing business in Arkansas, California, Connecticut, Kansas, Missouri, Nevada, Oklahoma, and Texas.

1.6   SBC-7STATE - As used herein, SBC-7STATE means the applicable above listed ILEC(s) doing business in Arkansas, California, Kansas, Missouri, Nevada, Oklahoma, and Texas.

1.7   SBC-SWBT - As used herein, SBC-SWBT means the applicable above listed ILEC(s) doing business in Arkansas, Kansas, Missouri, Oklahoma, and Texas.

1.8   SBC-AMERITECH - As used herein, SBC-AMERITECH means the applicable above listed ILEC(s) doing business in Illinois, Indiana, Michigan, Ohio, and Wisconsin.

1.9   PACIFIC - As used herein, PACIFIC means the applicable above listed ILEC doing business in California.

1.10   NEVADA - As used herein, NEVADA means the applicable above listed ILEC doing business in Nevada.

1.11   SNET - As used herein, SNET means the applicable above listed ILEC doing business in Connecticut.

1.12   LNP, DL and E911, when used in this Appendix, are limited exclusively to those services provided under this Agreement in conjunction with fixed wireless service offered in substantially the same technical manner provided by AWS or one of its affiliated wireless companies in one or more states as of the effective date of this Appendix.

2.   GENERAL CONDITIONS

2.1   On an interim basis, until the earlier of either (1) termination of the Agreement or (2) until such time as the FCC, the Commission or an appropriate court makes a determination (the enforcement of which is not stayed) that providers of fixed wireless service offered in substantially the same technical manner provided by AWS or one of its affiliated wireless companies in one or more states as of the effective date of this Appendix must be certified as competitive local exchange carriers or should be subject to substantially the same interconnection terms and conditions as wireline local exchange carriers, SBC-13STATE shall provide the OSS functions specified herein for LNP, DL and E911. SBC-13STATE expressly reserves all of its legal rights and expressly does not waive any position, particularly as to the appropriateness and legality of providing fixed wireless service as a CMRS provider and the need for a true-up to reflect the ultimate decision of applicable regulatory bodies as to how fixed wireless service should be provided by AWS. AWS should not assume that SBC-13STATE's willingness to provide OSS functions on an interim basis is any indication that SBC-13STATE believes that these arrangements are required by law or the Agreement or can be continued beyond the expiration of the Agreement. SBC-13STATE also fully reserves its rights, including but not limited to the right to pursue any regulatory, judicial or quasi-judicial action, to determine the appropriateness and legality of providing fixed wireless service in substantially the same technical manner provided by AWS or one of its affiliated wireless companies in one or more states as of the effective date of this Appendix as a CMRS provider.   AWS reserves all rights, including the right to pursue or contest before any regulatory, judicial, or quasi-judicial entity the services, terms and conditions contained in this Appendix, and reserves the right to assert that the terms and conditions agreed to on an interim basis by this Appendix are not applicable to AWS.

2.2   **Proper Use of OSS interfaces:**

2.2.1   For SBC-12STATE, AWS agrees to utilize SBC-12STATE electronic interfaces, as described herein, only for the purposes of establishing and maintaining LNP, DL and E911 through SBC-12STATE.   In addition, AWS agrees that such use will comply with the security provisions set out in Section 8 below.   Failure to comply with such security guidelines may result in forfeiture of electronic access to OSS functionality. In addition, AWS shall be responsible for and indemnifies SBC-12STATE against any cost, expense or liability relating to any unauthorized entry or access into, or use or manipulation of SBC-12STATE's OSS from AWS systems, workstations or terminals or by AWS employees or agents or any third party gaining access through information and/or facilities obtained from or utilized by AWS and shall pay SBC-12STATE for any and all damages caused by such unauthorized entry.

2.2.2   For SNET region, AWS agrees to access and utilize SNET's Enhanced Services Access Platform, (ESAP), only for the purposes described herein. AWS agrees that its access and use of ESAP shall, at all times, comport with SNET's "Wholesale CIWin User Guide", "EF User Guide", "ESAP Installation Guide", "ESAP Help Desk Guide", "CLEC Mechanized Interface Specification", and any other guide describing the interface or interface requirements that SNET may, from time to time, provide AWS (collectively, the "Guides").   Failure materially to adhere to any material provision of such Guides may result, among other things, in forfeiture of electronic access to SNET's OSS functionality via ESAP upon notice.   In addition, AWS shall be responsible for and indemnifies SNET against any cost, expense or liability relating to any unauthorized entry or access into, or use or manipulation of SNET's OSS or ESAP from AWS complimentary systems, workstations or terminals or by AWS employees or agents any third party gaining access through information and/or facilities obtained from or utilized by AWS and shall pay SNET for any and all damages caused by such unauthorized entry.

2.3   **Accessing Information via OSS**

2.3.1   The Parties acknowledge that information accessed via SBC-13STATE OSS may contain Customer Proprietary Network Information (CPNI). AWS may access Customer CPNI solely for pre-order and order purposes pursuant to the terms of this Appendix.   Accordingly, within SBC-13STATE regions, AWS access to pre-order functions will be limited to supporting the ordering by AWS of LNP.   AWS's access to pre-order functions described in Section 3 below will only be utilized to view CPNI of Customers where AWS has obtained Customer authorization as required under Applicable Laws.   Additionally, where such access occurs prior to conversion of the Customer to AWS, an authorization for release of CPNI from the Customer shall also be required prior to access to OSS.

The release of CPNI must adhere to all requirements of Applicable Law. The authorization for release of CPNI must substantially reflect the provisions of subsection 2.3.2. In SBC-7STATE, AWS may also access via OSS CPNI of end users of other Telecommunications Carriers that are listed in SBC-7STATE's databases by complying with the same terms and conditions as outlined above in this subsection 2.3.1 for accessing database information of Customers via OSS.

2.3.2 For SBC-13 STATE, "This written consent serves as instruction to all holders of any local exchange telecommunications Customer Proprietary Network Information ("CPNI") and account identification information to provide such information to AWS. Specifically, I authorize disclosure of any account billing name, billing address, and directory listing information, and CPNI, including, service address, service and feature subscription and long distance carrier identity. This Authorization remains in effect until such time as I [Name of Customer] revoke(s) it directly or appoint(s) another individual/company with such capacity or AWS receives notice to disconnect my local exchange service or notice that a service disconnect has been performed. At and from such time, this Authorization is null and void."

2.3.3 The following additional provisions apply in PACIFIC when AWS is serving residence Customers. For residence Customers, prior to accessing such information, AWS shall, on its own behalf and on behalf of PACIFIC, comply with all applicable requirements of Section 2891 of the California Public Utilities Code and 47 USC 222 (and implementing FCC decisions thereunder), and, where accessing such information via an electronic interface, AWS shall have obtained an authorization to become the Customer's local service provider. Accessing such information by AWS shall constitute certification that AWS is in compliance with applicable requirements of Section 2891 and Section 222 (and implementing FCC decisions thereunder) and has complied with the prior sentence. AWS shall receive and retain such information in conformance with the requirements of 47 USC 222 (and implementing FCC decisions thereunder). AWS agrees to indemnify, defend and hold harmless PACIFIC against any claim made by a residence Customer or governmental entity against PACIFIC or AWS under Section 2891 or Section 222 (and implementing FCC decisions thereunder) or for any breach by AWS of this Section 2.

2.3.4 Throughout SBC-13STATE region, AWS is solely responsible for determining whether proper authorization has been obtained and holds SBC-13STATE harmless from any loss on account of AWS's failure to obtain proper CPNI consent from a Customer.

2.4   By utilizing electronic interfaces to access OSS functions, AWS agrees to
        perform accurate and correct ordering as it relates to the application of rates and
        charges, subject to the terms of this Agreement and applicable tariffs dependent
        on region of operation. In addition, AWS agrees to perform accurate and correct
        ordering, dependent upon region of operation, pursuant to the terms of this
        Agreement. AWS is also responsible for all actions of its employees using any of
        SBC-13STATE's OSS systems.   As such, AWS agrees to accept and pay all
        reasonable costs or expenses, including labor costs, incurred by SBC-13STATE
        caused by any and all inaccurate ordering or usage of the OSS, if such costs are
        not already recovered through other charges assessed by SBC-13STATE to AWS.
        In addition, AWS agrees to indemnify and hold SBC-13STATE harmless against
        any claim made by an Customer of AWS or other third parties against SBC-
        13STATE caused by or related to AWS's use of any SBC-13STATE OSS. In
        addition, SBC-13STATE retains the right to audit all activities by AWS using any
        SBC-13STATE OSS solely for the purposes of ensuring compliance with the
        terms and conditions of this appendix. All such information obtained through an
        audit shall be deemed proprietary and shall be covered by the confidentiality
        provisions of the Agreement.

2.5   The Information Services (I.S.) Call Center for the SBC-8STATE region, and the
        Resource Center for the SBC-AMERITECH region provides for technical support
        function of electronic OSS interfaces. AWS will also provide a single point of
        contact for technical issues related to AWS's electronic interfaces.

2.6   SBC-13STATE will and AWS may participate in the Order and Billing Forum
        (OBF) and the Telecommunications Industry Forum (TCIF) to establish and
        conform to uniform industry guidelines for electronic interfaces for pre-order,
        ordering, and provisioning. Neither Party waives its rights as participants in such
        forums or in the implementation of the guidelines.   To achieve system
        functionality as quickly as possible, the Parties acknowledge that SBC-13STATE
        may deploy interfaces with requirements developed in advance of industry
        guidelines.   Thus, subsequent modifications may be necessary to comply with
        emerging guidelines.   AWS and SBC-13STATE are individually responsible for
        evaluating the risk of developing their respective systems in advance of
        guidelines and agree to support their own system modifications to comply with
        new requirements.

2.7   Due to enhancements and on-going development of access to SBC-13STATE's
        OSS functions, certain interfaces described in this Appendix may be modified,
        temporarily unavailable or may be phased out after execution of this Appendix.
        SBC-13STATE shall provide advance, written notice of interface phase-out.   In
        addition, SBC-13STATE shall provide at least 10 days advance, written notice of
        any scheduled OSS maintenance.

2.8   AWS is responsible for obtaining operating system software and hardware to
        access SBC-13STATE OSS functions as specified in: "Requirements for Access

to Southwestern Bell OSS Functions" and "Requirements for Access to Telco OSS Functions" and "SNET W-CIW in Installation Guide" and "Ameritech Electronic Service Order Guide", or any other documents or interface requirements subsequently generated by SBC-13STATE for any of its regions.

3.   **PRE-ORDERING**

3.1   SBC-13STATE will provide real time access to pre-order functions to support AWS ordering of LNP and DL. The Parties acknowledge that ordering requirements necessitate the use of current, real time pre-order information to accurately build service orders. The following list represents pre-order functions that are available to AWS so that AWS order requests may be created to comply with SBC-13STATE region-specific ordering requirements.

3.2   **Pre-ordering functions for LNP and DL:**

    3.2.1   Access to SBC-13STATE retail or resold CPNI and account information for pre-ordering will include: billing name, service address, billing address, service and feature subscription, directory listing information, long distance carrier identity, and for SBC-12STATE only, pending service order activity. AWS agrees that AWS's representatives will not access the information specified in this sub-Section 3.2.1 until AWS has obtained such Customer's authorization for release of CPNI, in accordance with the conditions as described in Section 2.3 of this Appendix**.**

    3.2.2   Service address verification.

3.3   **Electronic Access to Pre-Order Functions:**

    3.3.1   SNET LNP and DL Pre-Order System Availability. SNET will provide AWS access to the following system:

        3.3.1.1 MSAP, which is an Electronic Data Interchange (EDI) based interface which provides access to pre-order functions.

    3.3.2   SBC-AMERITECH LNP and DL Pre-Order System Availability. SBC-AMERITECH will provide AWS access to the following system:

        3.3.2.1 TCNet and EDI are available for the pre-ordering functions listed in Section 3.2

    3.3.3   SBC-7STATE LNP and DL Pre-order System Availability. SBC-7STATE will provide AWS access to the following systems:

        3.3.3.1 DataGate is a transaction-based data query system through which SBC-7STATE provides AWS access to pre-ordering functions.

This gateway shall be a Transmission Control Protocol/Internet Protocol (TCP/IP) gateway and will, once AWS has developed its own interface, allow AWS to access the pre-order functions for LNP and DL. An industry standard EDI/CORBA Pre-ordering Gateway is also provided by SBC-7STATE. This pre-ordering gateway supports two structural protocols, EDI and CORBA, as recommended by the technical industry committees. EDI/CORBA, like DataGate, is application-to-application interface that can be integrated with AWS's own negotiation system and that supports both LNP and DL. Where DataGate follows industry guidelines, but is based on SBC-7STATE's proprietary pre-ordering functionality, EDI/CORBA is an industry-wide standard pre-ordering interface.

3.3.3.2 Verigate is an interface developed by SBC-7STATE that provides access to the pre-ordering functions for LNP and DL. Verigate is accessible via Toolbar.

3.4 **Other Pre-order Function Availability:**

3.4.1 Upon request, but not more frequently than once a month, SBC-12STATES will provide AWS certain pre-order information in batch transmission for the purposes of back-up data for periods of system unavailability. Specifically, the Street Address Guide (SAG) may be electronically provided to support address verification. The Parties recognize such information must be used to construct order requests only in exception handling situations.

4. ORDERING/PROVISIONING

4.1 SBC-13STATE provides access to ordering functions (as measured from the time SBC-13STATE receives accurate service requests from the interface) to support AWS provisioning of LNP, DL and E911 via one or more electronic interfaces. DL includes directory assistance and white page listings. Ordering of LNP is through use of the number portability local service request, with or without DL. Ordering of DL without LNP is through use of the directory service request and directory listing request.

4.2 SBC-13STATE will provide AWS access to one or more of the following systems or interfaces:

4.2.1 **Ordering System Availability for LNP and DL in SBC-13STATE:**

4.2.1.1 SBC-13STATE makes available to AWS an Electronic Data Interchange (EDI) interface for transmission of SBC-13STATE ordering requirements via formats provided on the Local Service

Request (LSR) as defined by the OBF and via EDI mapping as defined by TCIF. In ordering and provisioning LNP and DL, AWS and SBC-13STATE will utilize industry guidelines developed by OBF and TCIF EDI to transmit data based upon SBC-13STATE's LNP and DL ordering requirements, dependent on operating region. For the SNET region, the EDI-based app-to-app interface is known as MSAP.

4.2.1.2 For SBC-SWBT and PACIFIC, LEX is an interface that provides access to the ordering functions for LNP and DL.

4.2.2 **Provisioning for LNP and DL in SBC-7STATE**: SBC-7STATE will provision LNP and DL as detailed in AWS order requests. Access to status on such orders will be provided via the following electronic interfaces:

4.2.2.1 Order Status will allow AWS to check service order status. Order Status and Provisioning Order Status are both accessible via SBC-7STATE Toolbar.

4.2.2.2 For EDI ordering, SBC-7STATE will provide, and AWS shall use, an EDI interface for transferring and receiving orders, Firm Order Confirmation (FOC), service completion, and, as available, other provisioning data and information. SBC-7STATE will provide AWS with a FOC for each LNP and DL request.

4.2.3 **Provisioning for LNP and DL in SBC-AMERITECH and SNET**: SBC-AMERITECH and SNET will provision LNP and DL as detailed in AWS order requests. Access to status on such orders will be provided via the following electronic interfaces:

4.2.3.1 For EDI ordering, SBC-AMERITECH and SNET provide AWS, and AWS shall use, an EDI interface for transferring and receiving orders, FOC, Service Order Completion (SOC), and, as available, other provisioning data and information. SBC-AMERITECH and SNET will provide AWS with a FOC for each LNP and DL request.

4.2.4 **E911 in PACIFIC**: For PACIFIC only, E911 Gateway is available for updating the E911 database, and allows AWS to provide updates to the E911 system for AWS's Customers. A separate telephone number ("TN") Query function is also available to allow AWS to verify E911 data on file for their Customers.

5. **MAINTENANCE/REPAIR**

5.1 Real time electronic interfaces are accessible in each region to place, and check

the status of, trouble reports for LNP. Upon request, AWS may access these functions via the following methods:

5.1.1   In SBC-7STATE, Trouble Administration (TA) system access provides AWS with SBC-7STATE software that allows AWS to submit trouble reports and subsequently check status on trouble reports for AWS Customers. TA is accessible via SBC-7STATE Toolbar.

5.1.2   In PACIFIC and NEVADA, Telco Service Manager (PBSM) allows AWS to issue and view status of trouble tickets.

5.1.3   In SBC-AMERITECH, Electronic Bonding for Trouble Administration (EBTA-GUI) allows AWS to issue and view trouble tickets.

5.1.4   In SNET the maintenance and repair functionality for LNP is available via the MSAP EDI interface.

5.1.5   In SBC-12STATE, Electronic Bonding Interface (EBI) is an interface that is available for trouble report submission and status updates. EBI conforms to ANSI guidelines T1.227:1995 and T1.228:1995, Electronic Communications Implementation Committee (ECIC) Trouble Report Format Definition (TFRD) Number 1 as defined in ECIC document ECIC/TRA/95-003, and all guidelines referenced within those documents, as mutually agreed upon by AWS and SBC-12STATE.   Functions currently implemented include Enter Trouble, Request Trouble Report Status, Add Trouble Information, Modify Trouble Report Attributes, Trouble Report Attribute Value Change Notification, and Cancel Trouble Report, as explained in 6 and 9 of ANSI T1.228:1995. AWS and SBC-12STATE will exchange requests over a mutually agreeable X.25-based network.

6.   BILLING

6.1   Billing for DL will be available via paper in all regions due to the various billing systems under which they are currently billed. DL is billed out of the LSB (LEC Services Billing) system for SBC-AMERITECH region and out of the IBIS Billing system in SBC-SWBT. Paper bills are the only option for billing format for DL in these two regions. DL is billed out of CABS in SNET, NEVADA and PACIFIC and is available via paper or magnetic tape. This magnetic tape option in the SNET, NEVADA and PACIFIC regions is known as Bill Data Tape. The local Bill Data Tape contains the same information that would appear on AWS's paper bill.

7.   REMOTE ACCESS FACILITY

7.1   For the SBC-SWBT region, AWS must access the following OSS interfaces via a Local Remote Access Facility (LRAF) located in Dallas, Texas: DataGate; EDI-Ordering; Electronic Bonding via EDI/SSL or CORBA; and via Toolbar, Trouble Administration, Order Status, Provisioning Order Status, Verigate and LEX. Connection to the LRAF will be established via a "port" either through dial-up or direct connection as described in Section 7.3. AWS may utilize a port to access these interfaces to perform the supported functions in any SBC-SWBT state where AWS has executed an Appendix OSS.

7.2   In PACIFIC and NEVADA regions, AWS must access the following OSS interfaces via a Pacific Remote Access Facility (PRAF) located in Fairfield, California: DataGate; EDI-Ordering; Electronic Bonding via EDI/SSL or CORBA; and via Toolbar Verigate, LEX, Order Status, PBSM, and Provisioning Order Status. Connection to the PRAF will be established via a "port" either through dial-up or direct connection as described in Section 7.3. AWS may utilize a port to access these interfaces to perform the supported functions in PACIFIC or NEVADA where AWS has executed an Appendix OSS and purchases System Access in that state.

7.3   For SBC-7STATE, AWS may use three types of access: Switched, Private Line, and Frame Relay. For Private Line and Frame Relay "Direct Connections," AWS shall provide its own router, circuit, and two Channel Service Units/Data Service Units (CSU/DSU). The demarcation point shall be the router interface at the LRAF and/or PRAF. Switched Access "Dial-up Connections" require AWS to provide its own modems and connection to the SBC-SWBT LRAF and the PACIFIC PRAF. AWS shall pay the cost of the call if Switched Access is used.

7.4   For SBC-7STATE, AWS shall use TCP/IP to access SBC-7STATE OSS via the LRAF and the PRAF. In addition, AWS shall have one valid Internet Protocol (IP) network address per region. AWS shall maintain a user-id / password unique to each individual for accessing a SBC-SWBT OSS and PACIFIC OSS on AWS's behalf. AWS shall provide estimates regarding its volume of transactions, number of concurrent users, desired number of private line or dial-up (switched) connections, and length of a typical session.

7.5   For SBC-7STATE, AWS shall attend and participate in implementation meetings to discuss AWS LRAF/PRAF access plans in detail and schedule testing of such connections.

7.6   For SBC-AMERITECH, AWS may use four types of access: DSO (56KB), DS1 (1.5MB), dedicated and Frame Relay (DS0 and DS1). AWS shall provide its own router, circuit, and two Channel Service Units/Data Service Units (CSU/DSU). AWS must use a legal IP address for its end of the connection.

7.7   For SNET region, AWS may use a private line connection. AWS shall provide and maintain its own router and CSU/DSU.

8. DATA CONNECTION SECURITY REQUIREMENTS

8.1   AWS agrees that interconnection of AWS data facilities with SBC-13STATE data facilities for access to OSS will be in compliance with SBC-13STATE's Competitive Local Exchange Carrier (CLEC) Operations Support System Interconnection Procedures document current at the time of initial connection to a RAF. The following additional terms in this Section 8 govern direct and dial up connections between AWS and the PRAF and LRAF for access to OSS Interfaces.

8.2   **Joint Security Requirements**

8.2.1   Both Parties will maintain accurate and auditable records that monitor user authentication and machine integrity and confidentiality (e.g., password assignment and aging, chronological logs configured, system accounting data, etc.)

8.2.2   Both Parties shall maintain accurate and complete records detailing the individual data connections and systems to which they have granted the other Party access or interface privileges. These records will include, but are not limited to, user ID assignment, user request records, system configuration, time limits of user access or system interfaces. These records should be kept until the termination of this Agreement or the termination of the requested access by the identified individual. Either Party may initiate a compliance review of the connection records to verify that only the agreed to connections are in place and that the connection records are accurate.

8.2.3   Each Party shall notify the other party immediately, upon termination of employment of an individual user with approved access to the other Party's network.

8.2.4   Both Parties shall use an industry standard virus detection software program at all times. The Parties shall immediately advise each other by telephone upon actual knowledge that a virus or other malicious code has been transmitted to the other Party.

8.2.5   All physical access to equipment and services required to transmit data will be in secured locations. Verification of authorization will be required for access to all such secured locations. A secured location is where walls and doors are constructed and arranged to serve as barriers and to provide uniform protection for all equipment used in the data connections which are made as a result of the user's access to either AWS's or SBC-13STATE's network. At a minimum, this shall include: access doors equipped with card reader control or an equivalent authentication procedure and/or device, and egress doors which generate a real-time

alarm when opened and which are equipped with tamper resistant and panic hardware as required to meet building and safety standards.

8.2.6   Both Parties shall maintain accurate and complete records on the card access system or lock and key administration to the rooms housing the equipment utilized to make the connection(s) to the other Party's network. These records will include management of card or key issue, activation or distribution and deactivation.

8.3   **Additional Responsibilities of Both Parties**

8.3.1   Modem/DSU Maintenance And Use Policy: To the extent the access provided hereunder involves the support and maintenance of AWS equipment on SBC-13STATE's premises, such maintenance will be provided under the terms of the Competitive Local Exchange Carrier (CLEC) Operations Support System Interconnection Procedures document cited above.

8.3.2   Monitoring: Each Party will monitor its own network relating to any user's access to the Party's networks, processing systems, and applications. This information may be collected, retained, and analyzed to identify potential security risks without notice. This information may include, but is not limited to, trace files, statistics, network addresses, and the actual data or screens accessed or transferred.

8.3.3   Each Party shall notify the other Party's security organization immediately upon initial discovery of actual or suspected unauthorized access to, misuse of, or other "at risk" conditions regarding the identified data facilities or information. Each Party shall provide a specified point of contact. If either Party suspects unauthorized or inappropriate access, the Parties shall work together to isolate and resolve the problem.

8.3.4   In the event that one Party identifies inconsistencies or lapses in the other Party's adherence to the security provisions described herein, or a discrepancy is found, documented, and delivered to the non-complying Party, a corrective action plan to address the identified vulnerabilities must be provided by the non-complying Party within thirty (30) calendar days of the date of the identified inconsistency. The corrective action plan must identify what will be done, the Party accountable/responsible, and the proposed compliance date. The non-complying Party must provide periodic status reports (minimally monthly) to the other Party's security organization on the implementation of the corrective action plan in order to track the work to completion.

8.3.5   In the event there are technological constraints or situations where either Party's corporate security requirements cannot be met, the Parties will

institute mutually agreed upon alternative security controls and safeguards to mitigate risks.

8.3.6 All network-related problems will be managed to resolution by the respective organizations, AWS or SBC-13STATE, as appropriate to the ownership of a failed component. As necessary, AWS and SBC-13STATE will work together to resolve problems where the responsibility of either Party is not easily identified.

8.4 **Information Security Policies And Guidelines For Access To Computers, Networks and Information By Non-Employee Personnel:**

8.4.1 Information security policies and guidelines are designed to protect the integrity, confidentiality and availability of computer, networks and information resources. Sections 8.5 - 8.11 summarize the general policies and principles for individuals who are not employees of the Party that provides the computer, network or information, but have authorized access to that Party's systems, networks or information. Questions should be referred to AWS or SBC-13STATE, respectively, as the providers of the computer, network or information in question.

8.4.2 It is each Party's responsibility to notify its employees, contractors and vendors who will have access to the other Party's network, on the proper security responsibilities identified within this Attachment. Adherence to these policies is a requirement for continued access to the other Party's systems, networks or information. Exceptions to the policies must be requested in writing and approved by the other Party's information security organization.

8.5 **General Policies**

8.5.1 Each Party's resources are for approved business purposes only.

8.5.2 Each Party may exercise at any time its right to inspect, record, and/or remove all information contained in its own systems, and take appropriate action should unauthorized or improper usage be discovered

8.5.3 Individuals will only be given access to resources that they are authorized to receive and which they need to perform their job duties. Users must not attempt to access resources for which they are not authorized.

8.5.4 Authorized users must not develop, copy or use any program or code which circumvents or bypasses system security or privilege mechanism or distorts accountability or audit mechanisms.

8.5.5 Actual or suspected unauthorized access events must be reported immediately to each Party's security organization or to an alternate

contact identified by that Party.   Each Party shall provide its respective security contact information to the other.

8.6 **User Identification**

8.6.1 Access to each Party's corporate resources will be based on identifying and authenticating individual users in order to maintain clear and personal accountability for each user's actions.

8.6.2 User identification shall be accomplished by the assignment of a unique, permanent user id, and each user id shall have an associated identification number for security purposes.

8.6.3 User ids will be revalidated on a monthly basis.

8.7 **User Authentication**

8.7.1 Users will usually be authenticated by use of a password.   Strong authentication methods (e.g. one-time passwords, digital signatures, etc.) may be required in the future.

8.7.2 Passwords must not be stored in script files.

8.7.3 Passwords must be entered by the user in real time.

8.7.4 Passwords must be at least 6-8 characters in length, not blank or a repeat of the user id; contain at least one letter, and at least one number or special character must be in a position other than the first or last one. This format will ensure that the password is hard to guess. Most systems are capable of being configured to automatically enforce these requirements. Where a system does not mechanically require this format, the users must manually follow the format.

8.7.5 Systems will require users to change their passwords regularly (usually every 31 days).

8.7.6 Systems are to be configured to prevent users from reusing the same password for 6 changes/months.

8.7.7 Personal passwords must not be shared. A user who has shared his password is responsible for any use made of the password.

8.8 **Access and Session Control**

8.8.1 Destination restrictions will be enforced at remote access facilities used for access to OSS Interfaces. These connections must be approved by each Party's corporate security organization.

8.8.2   Terminals or other input devices must not be left unattended while they may be used for system access. Upon completion of each work session, terminals or workstations must be properly logged off.

8.9   **User Authorization**

8.9.1   On the destination system, users are granted access to specific resources (e.g. databases, files, transactions, etc.). These permissions will usually be defined for an individual user (or user group) when a user id is approved for access to the system.

8.10   **Software And Data Integrity**

8.10.1   Each Party shall use a comparable degree of care to protect the other Party's software and data from unauthorized access, additions, changes and deletions as it uses to protect its own similar software and data. This may be accomplished by physical security at the work location and by access control software on the workstation.

8.10.2   Untrusted software or data shall be scanned for viruses before use on a Party's corporate facilities that can be accessed through the direct connection or dial up access to OSS interfaces.

8.10.3   Unauthorized use of copyrighted software is prohibited on each Party's corporate systems that can be access through the direct connection or dial up access to OSS Interfaces.

8.10.4   Proprietary software or information (whether electronic or paper) of a Party shall not be given by the other Party to unauthorized individuals. When it is no longer needed, each Party's proprietary software or information shall be returned by the other Party or disposed of securely. Paper copies shall be shredded. Electronic copies shall be overwritten or degaussed.

8.11   **Monitoring And Audit**

8.11.1   To deter unauthorized access events, a warning or no trespassing message will be displayed at the point of initial entry (i.e., network entry or applications with direct entry points).   Each Party should have several approved versions of this message. Users should expect to see a warning message similar to this one:
"This is a (SBC-13STATE or AWS) system restricted to Company official business and subject to being monitored at any time. Anyone using this system expressly consents to such monitoring and to any evidence of unauthorized access, use, or modification being used for criminal prosecution."

8.11.2 After successful authentication, each session will display the last logon date/time and the number of unsuccessful logon attempts. The user is responsible for reporting discrepancies.

9. OPERATIONAL READINESS TEST (ORT) FOR ORDERING/PROVISIONING AND REPAIR/ MAINTENANCE INTERFACES

9.1 Prior to live access to interface functionality, the Parties must conduct Operational Readiness Testing (ORT), which will allow for the testing of the systems, interfaces, and processes for the OSS functions. ORT will be completed in conformance with agreed upon processes and implementation dates.

9.2 Prior to live system usage, AWS must complete user education classes for SBC-13STATE-provided interfaces that affect the SBC-13STATE network. Course descriptions for all available classes by region are posted on the CLEC website in the Customer Education section. CLEC Training schedules by region are also available on the CLEC website and are subject to change, with class lengths varying. Classes are train-the-trainer format to enable AWS to devise its own course work for its own employees. Charges as specified below will apply for each class:

Training Rates	5 day class	4.5 day class	4 day class	3.5 day class	3 day class	2.5 day class	2 day class	1.5 day class	1 day class	1/2 day class
1 to 5 students	$4,050	$3,650	$3,240	$2,835	$2,430	$2,025	$1,620	$1,215	$810	$405
6 students	$4,860	$4,380	$3,890	$3,402	$2,915	$2,430	$1,945	$1,455	$970	$490
7 students	$5,670	$5,100	$4,535	$3,969	$3,400	$2,835	$2,270	$1,705	$1,135	$570
8 students	$6,480	$5,830	$5,185	$4,536	$3,890	$3,240	$2,590	$1,950	$1,300	$650
9 students	$7,290	$6,570	$5,830	$5,103	$4,375	$3,645	$2,915	$2,190	$1,460	$730
10 students	$8,100	$7,300	$6,480	$5,670	$4,860	$4,050	$3,240	$2,430	$1,620	$810
11 students	$8,910	$8,030	$7,130	$6,237	$5,345	$4,455	$3,565	$2,670	$1,780	$890
12 students	$9,720	$8,760	$7,780	$6,804	$5,830	$4,860	$3,890	$2,920	$1,945	$970

9.3 A separate agreement will be required as a commitment to pay for a specific number of AWS students in each class. AWS agrees that charges will be billed by SBC-13STATE and AWS payment is due thirty (30) days following the bill date. AWS agrees that personnel from other competitive Local Service Providers may be scheduled into any class to fill any seats for which AWS has not contracted. Class availability is first-come, first served with priority given to AWS who have not yet attended the specific class.

9.4 Class dates will be based upon SBC-13STATE availability and will be coordinated among AWS, AWS's SBC-13STATE Account Manager, and SBC-13STATE Industry Markets CLEC Training Product Management.

9.5 AWS agrees to pay the cancellation fee of the full price noted in the separate agreement if AWS cancels scheduled classes less than two (2) weeks prior to the scheduled start date. AWS agrees to provide to SBC-13STATE completed

registration forms for each student no later than one week prior to the scheduled training class.

9.6   AWS agrees that AWS personnel attending classes are to utilize only training databases and training presented to them in class. Attempts to access any other SBC-13STATE system are strictly prohibited.

9.7   AWS further agrees that training material, manuals and instructor guides can be duplicated only for internal use for the purpose of training employees to utilize the capabilities of SBC-13STATE's OSS in accordance with this Appendix and shall be deemed "Confidential" information and subject to the terms, conditions and limitations of Section 20 of the Agreement.

10.   TERM

10.1   The term of this Appendix shall be until the first to occur of (i) the termination of this Agreement or (ii) the FCC, the Commission or an appropriate court makes a determination (the enforcement of which is not stayed) that providers of fixed wireless service offered in the manner that AWS or one of its affiliated wireless companies provides or intends to provide that service as of the effective date of this Appendix must be certified as competitive local exchange carriers or should be subject to substantially the same interconnection terms and conditions as wireline local exchange carriers.